

Planar polynomials and an extremal problem of Fischer and Matoušek

Robert S. Coulter* Rex W. Matthews† Craig Timmons‡

February 7, 2017

Abstract

Let G be a 3-partite graph with k vertices in each part and suppose that between any two parts, there is no cycle of length four. Fischer and Matoušek asked for the maximum number of triangles in such a graph. A simple construction involving arbitrary projective planes shows that there is such a graph with $(1 - o(1))k^{3/2}$ triangles, and a double counting argument shows that one cannot have more than $(1 + o(1))k^{7/4}$ triangles. Using affine planes defined by specific planar polynomials over finite fields, we improve the lower bound to $(1 - o(1))k^{5/3}$.

1 Introduction

Let n and k be positive integers and write $[n]$ for $\{1, 2, \dots, n\}$. If \mathcal{F} is a family of functions from $[n]$ to $[2]$, then a set $A \subseteq [n]$ is called *shattered* if given any function $g : A \rightarrow \{1, 2\}$, there exists a function $f \in \mathcal{F}$ such that $f(a) = g(a)$ for all $a \in A$. The well-studied *Vapnik-Chervonenkis dimension* or *VC-dimension* of \mathcal{F} is the maximum size of a subset $A \subseteq X$ that is shattered by \mathcal{F} . A generalization of VC-dimension is the so-called Natarajan dimension. Let \mathcal{F} be a collection of functions from $[n]$ to $[k]$. Given a set $A \subseteq [n]$, we say that A is *2-shattered* if for each $x \in A$, there is a pair $V_x \subseteq [k]$ such that for any choice of elements $c_x \in V_x$, there is an $f \in \mathcal{F}$ such that $f(x) = c_x$ for all $x \in A$. The family \mathcal{F} has *Natarajan dimension at most d* if there is no subset $A \subseteq X$ with $d + 1$ elements that is 2-shattered by \mathcal{F} .

A natural question is given n and d , how many functions can belong to \mathcal{F} if the VC-dimension of \mathcal{F} is at most d ? Similarly, given n , k , and d , one can ask how large \mathcal{F} can be if the Natarajan dimension of \mathcal{F} is at most d . Fischer and Matoušek [6] reformulated this problem as an interesting problem in extremal graph theory. Given a collection of functions \mathcal{F} from $[n]$ to $[k]$, we can view \mathcal{F} as defining a

*Department of Mathematical Sciences, University of Delaware, Newark, DE, 19716, USA.

†6 Earl St., Sandy Bay, Tasmania 7005, Australia.

‡Department of Mathematics and Statistics, California State University Sacramento, USA. craig.timmons@csus.edu. This author was supported by the Simons Foundation (Grant #359419)

n -uniform n -partite hypergraph where each part has k vertices. The vertex set of this hypergraph is $[n] \times [k]$ and the edges are all sets of the form

$$\{(1, f(1)), (2, f(2)), \dots, (n, f(n))\},$$

where $f \in \mathcal{F}$. A set $A \subseteq [n]$ is 2-shattered if the subhypergraph of \mathcal{F} induced by $A \times [k]$ contains a complete $|A|$ -uniform, $|A|$ -partite hypergraph with two vertices in each part. For more on VC-dimension, Natarajan dimension, and its connection to hypergraphs, we refer the reader to [6] and the references therein.

Fischer and Matoušek showed that there is a family of functions from $[n]$ to $[3]$ with $3n$ elements and Natarajan dimension 1. Additionally, the $3n$ is best possible. This gives a solution to a special case of the above mentioned problem, but many cases remain open. One of particular interest, mentioned explicitly in [6], is when $n = 3$, $d = 1$, and $k \geq 3$ is arbitrary. The corresponding extremal graph theory problem is as follows.

Problem 1.1 *Let G be a 3-partite graph with k vertices in each part and suppose that the bipartite graph between any two parts does not contain a cycle of length four. Determine how many triangles can appear in such a graph.*

While Problem 1.1 arose in the context of Natarajan dimension, given the recent activity on counting copies of a fixed graph H in an F -free graph with n vertices [2, 3, 7, 8, 9], it is an interesting extremal problem in its own right. Let

$$\Delta(k)$$

be the maximum number of triangles in a 3-partite graph with k vertices in each part such that between any two parts, there is no cycle of length four. To our knowledge, the best known bounds on $\Delta(k)$ are given in the next proposition.

Proposition 1.2 (Fischer, Matoušek [6]) *The function $\Delta(k)$ satisfies*

$$k^{3/2} - o(k^{3/2}) \leq \Delta(k) \leq k^{7/4} + O(k^{3/2})$$

as $k \rightarrow \infty$.

For a proof of the upper bound, see [6]. Our main result concerns the lower bound so we take a moment to sketch a proof. Assume that q is a power of a prime. Let $G(A, B)$ be the incidence graph of a projective plane of order q and let C be a set of $q^2 + q + 1$ vertices disjoint from $A \cup B$. Make a single vertex in C adjacent to all vertices in A and all vertices in B . This graph will be 3-partite with $q^2 + q + 1$ vertices in each part. There will be no cycle of length four between any two parts. The number of triangles in this graph is the number of edges between A and B which is $(q + 1)(q^2 + q + 1)$. Therefore,

$$\Delta(q^2 + q + 1) \geq (q + 1)(q^2 + q + 1)$$

whenever q is a power of a prime. Our main result improves this lower bound.

Theorem 1.3 *If q is a power of an odd prime, then*

$$\Delta(q^6) \geq q^6(q^3 - 1)(q + 1).$$

By Theorem 1.3 and a standard density of primes argument, we have

$$\Delta(k) \geq (1 - o(1))k^{5/3}$$

as $k \rightarrow \infty$.

To prove Theorem 1.3, we will use planar polynomials. Planar functions were introduced by Dembowski and Ostrom [5] in order to construct affine planes with certain collineation groups. Before defining planar polynomials, we introduce some notation. We write \mathbb{F}_q for the finite field with q elements and \mathbb{F}_q^\star for the nonzero elements of \mathbb{F}_q . The norm and trace maps from \mathbb{F}_{q^3} to \mathbb{F}_q will be denoted by N and Tr , respectively; that is, $x \in \mathbb{F}_{q^3}$,

$$N(x) = x^{1+q+q^2} \quad \text{and} \quad \text{Tr}(x) = x + x^q + x^{q^2}.$$

Assume now that q is a power of an odd prime. A polynomial $f \in \mathbb{F}_q[X]$ is a *planar polynomial* if, for each $a \in \mathbb{F}_q^\star$, the map

$$x \mapsto f(x+a) - f(x)$$

is a bijection on \mathbb{F}_q . Such polynomials can be used to construct affine planes and consequently, they can also be used to construct bipartite graphs without a cycle of length four. The simplest example of a planar polynomial is $f(X) = X^2$, and this is the smallest example of a class of planar monomials. Let α, e be positive integers. The monomial $f(X) = X^{q^\alpha+1}$ is planar over \mathbb{F}_{q^e} if and only if $\frac{e}{\gcd(\alpha, e)}$ is odd, see [4]. To obtain our lower bound, we consider planar monomials whose degree increases with q , specifically the monomial X^{q+1} over \mathbb{F}_{q^3} . The crucial algebraic ingredient used to prove Theorem 1.3 is derived from considering our graph construction using these monomials and may be of independent interest. It reads as follows.

Theorem 1.4 *Let q be a power of an odd prime. For any $a \in \mathbb{F}_{q^3}^\star$, the polynomial*

$$f_a(X) = X^{q+1} + a^{-1}(X^q + X) + N(a^{-1})(\text{Tr}(a) - 2a)$$

splits completely in $\mathbb{F}_{q^3}^\star$. Furthermore, if $a \in \mathbb{F}_q^\star$, then $f_a(X)$ has a single root of multiplicity $q+1$, and if $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, then the roots of $f_a(X)$ are all distinct.

The graph proving the lower bound in Theorem 1.3 is a 3-partite graph with q^6 vertices in each part, and the edge density between any two parts will be very close to $\frac{1}{q^3}$. If we treated the edges as if they were placed randomly, we would expect roughly q^9 triangles, however, this graph contains at least $q^{10} - O(q^9)$ triangles. This is significantly more triangles than one might expect and yet, the edges between the parts cannot be too unevenly distributed by the Expander Mixing Lemma.

In the next section we prove Theorem 1.4. The graph showing the lower bound of Theorem 1.3 is defined in Section 3, which also contains the proof of Theorem 1.3.

2 Proof of Theorem 1.4

The edges in the graph that we construct will be defined using the polynomial $X^{q+1} \in \mathbb{F}_{q^3}[X]$. Since this polynomial is planar, we will satisfy the condition of having no cycle of length four between two parts as the bipartite subgraph between any two parts is an affine plane. The difficult part is in counting the triangles. This is where we require Theorem 1.4 which we now prove.

Proof of Theorem 1.4. Let $a \in \mathbb{F}_{q^3}^*$ and

$$f_a(X) = X^{q+1} + a^{-1}(X^q + X) + N(a^{-1})(\text{Tr}(a) - 2a).$$

We first note that

$$\begin{aligned} f_a(-a^{-q}) &= a^{-q^2-q} - a^{-q^2-1} - a^{-q-1} + a^{-q^2-q-1}(a^{q^2} + a^q - a) \\ &= a^{-q^2-q} - a^{-q^2-1} - a^{-q-1} + a^{-q-1} + a^{-q^2-1} - a^{-q^2-q} \\ &= 0, \end{aligned}$$

so that $-a^{-q}$ is a root of $f_a(X)$. We now normalise $f_a(X)$ with respect to this root. We have

$$\begin{aligned} f_a(X - a^{-q}) &= (X^q - a^{-q^2})(X - a^{-q}) + a^{-1}(X^q + X) \\ &\quad - a^{-1}(a^{-q^2} + a^{-q}) + N(a^{-1})(\text{Tr}(a) - 2a) \\ &= X^{q+1} + X^q(a^{-1} - a^{-q}) + X(a^{-1} - a^{-q^2}) + f_a(-a^{-q}) \\ &= X^{q+1} + X^q(a^{-1} - a^{-q}) + X(a^{-1} - a^{-q^2}) \\ &= X \left(X^q + X^{q-1}(a^{-1} - a^{-q}) + (a^{-1} - a^{-q^2}) \right). \end{aligned}$$

Set $h(X) = X^q + X^{q-1}(a^{-1} - a^{-q}) + (a^{-1} - a^{-q^2})$, so that $f_a(X - a^{-q}) = X h(X)$.

The root $-a^{-q}$ will be a multiple root of $f_a(X)$ if and only if 0 is a root of $h(X)$. This occurs only when $a \in \mathbb{F}_q^*$, in which case $h(X) = X^q$. Consequently, $f_a(X) = (X + a^{-q})^{q+1}$, which establishes Theorem 1.4 in the case that $a \in \mathbb{F}_q^*$.

For the remainder of the proof, assume $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$. We know from the above discussion that $-a^{-q}$ is not a multiple root of $f_a(X)$. The reciprocal polynomial of $h(X)$ is

$$X^q h(X^{-1}) = (a^{-1} - a^{-q^2})X^q + (a^{-1} - a^{-q})X + 1.$$

Let $L(X) = (a^{-1} - a^{-q^2})X^q + (a^{-1} - a^{-q})X$. The polynomial $L(X)$ is a linearized polynomial, and as it has a non-zero X term, it has no multiple roots. (For this and many other results on linearized polynomials, see Lidl and Niederreiter [10], Chapter 3.) Indeed, it can be seen from the identity

$$\begin{aligned} L(X) &= (a^{-1} - a^{-q^2})X^q + (a^{-1} - a^{-q})X \\ &= (a^{-1} - a^{-q^2})X^q - (a^{-1} - a^{-q^2})^q X, \end{aligned}$$

that $L(X)$ splits completely in \mathbb{F}_{q^3} , its roots being given by $x = \alpha(a^{-1} - a^{-q^2})$, with $\alpha \in \mathbb{F}_q$. Using the additive properties of linearized polynomials, it follows that if $x_c \in \mathbb{F}_{q^3}$ satisfies $L(x_c) = c$ for some $c \in \mathbb{F}_{q^3}$, then $L(x_c + \alpha(a^{-1} - a^{-q^2})) = c$ for

any $\alpha \in \mathbb{F}_q$. Thus, if $L(X) - c$ has a root in \mathbb{F}_{q^3} , then it splits completely over \mathbb{F}_{q^3} with distinct roots. Given the relationship between $f_a(X)$, $h(X)$ and $L(X)$, we therefore have $f_a(X)$ splits completely, with distinct roots, over \mathbb{F}_{q^3} if and only if $L(X) + 1$ has a root in \mathbb{F}_{q^3} . We will show something stronger; we shall prove that for any $\alpha \in \mathbb{F}_q$, $L(X) - \alpha$ splits completely, with distinct roots, in \mathbb{F}_{q^3} .

Fix $\alpha \in \mathbb{F}_q$ and suppose $L(x) = \alpha$ holds for some $x \in \mathbb{F}_{q^3}$. Then $L(x)^q = \alpha$ also. Hence,

$$\begin{aligned} 0 &= L(x)^q - L(x) \\ &= (a^{-q} - a^{-1})x^{q^2} + (a^{-q} - a^{-q^2})x^q - (a^{-1} - a^{-q^2})x^q - (a^{-1} - a^{-q})x \\ &= (a^{-q} - a^{-1})(x^{q^2} + x^q + x) \\ &= (a^{-q} - a^{-1})\text{Tr}(x), \end{aligned}$$

and so $\text{Tr}(x) = 0$. This argument can be reversed, proving $L(x) \in \mathbb{F}_q$ if and only if $\text{Tr}(x) = 0$. As there are q^2 elements $x \in \mathbb{F}_{q^3}$ for which $\text{Tr}(x) = 0$, we know that, counting multiplicities, $L(x) \in \mathbb{F}_q$ for q^2 choices of x . However, the degree of $L(X)$ is q , and so the polynomial $L(X) - \alpha$ can have at most q roots for any fixed $\alpha \in \mathbb{F}_q$. Since we have exactly q choices for $\alpha \in \mathbb{F}_q$, the polynomial $L(X) - \alpha$ must have exactly q distinct roots for each $\alpha \in \mathbb{F}_q$. In particular, $L(X) + 1$ does, proving that $f_a(X)$ has $q + 1$ distinct roots whenever $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$. ■

3 Proof of Theorem 1.3

We begin this section by defining the graph that implies the lower bound asserted by Theorem 1.3.

The Construction: Let q be a power of an odd prime. Choose $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ so that

$$aN(a^{-1})(\text{Tr}(a) - 2a) - 1 \neq 0 \quad (1)$$

and -1 is not a root of $f_a(X)$. The equation $aN(a^{-1})(\text{Tr}(a) - 2a) - 1 = 0$ is equivalent to

$$(a^{-1})^{q^2+q-1} + (a^{-1})^{q^2} + (a^{-1})^q - 1 = 0$$

so there are at most $q^2 + q - 1$ elements of $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ for which (1) fails. Similarly, -1 is a root of $f_a(X)$ if and only if a^{-1} is a root of $X^{q^2+q} - X^{q^2+1} - X^{q+1} + 2X - 1$. Since $q^3 - q - (q^2 + q) - (q^2 + q - 1) \geq 1$ for all $q \geq 3$, such an a exists. We also remark that since $a \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, 0 is not a root of $f_a(X)$ as $0 = f_a(0)$ implies that $\text{Tr}(a) = 2a$ which, in turn, implies $a \in \mathbb{F}_q$.

Let

$$f(X) = (a - 1)X^{q+1}, \quad g(X) = (aN(a^{-1})(\text{Tr}(a) - 2a) - 1)X^{q+1}, \quad \text{and} \quad h(X) = X^{q+1}.$$

Each of the polynomials $f(X)$, $g(X)$, and $h(X)$ are nonzero planar polynomials over \mathbb{F}_{q^3} . Let A , B , and C be disjoint copies of $\mathbb{F}_{q^3} \times \mathbb{F}_{q^3}$. Elements in A are denoted by $(x, y)_A$ and the same goes for elements in B and C . Let $G_q(a)$ be the graph whose vertex set is $A \cup B \cup C$, where for all $x, y \in \mathbb{F}_{q^3}$ and $z \in \mathbb{F}_{q^3}^*$,

- $(x, y)_A$ is adjacent to $(x + z, y + f(z))_B$,

- $(x, y)_B$ is adjacent to $(x + z, y + g(z))_C$, and
- $(x, y)_C$ is adjacent to $(x + z, y + h(z))_A$.

Using Theorem 1.4, we now prove the following which implies Theorem 1.3.

Theorem 3.1 *The graph $G_q(a)$ is a 3-partite graph with q^6 vertices in each part and there is no cycle of length four between two parts. Furthermore, the number of triangles in $G_q(a)$ is at least $q^6(q^3 - 1)(q + 1)$.*

Proof. It is clear that $G_q(a)$ is 3-partite with q^6 vertices in each part. Since each of f , g , and h are planar polynomials, there is no cycle of length four between any two parts. This is easily deduced from Lemma 12 of [5]. It remains to show that $G_q(a)$ has at least $q^6(q^3 - 1)(q + 1)$ triangles.

Let ξ_1, \dots, ξ_{q+1} be distinct roots in \mathbb{F}_{q^3} of

$$X^{q+1} + a^{-1}(X^q + X) + N(a^{-1})(\text{Tr}(a) - 2a).$$

These roots exist by Theorem 1.4. Choose a root ξ_j and let z_2 be any element of $\mathbb{F}_{q^3}^*$. Define z_1 by $z_1 = \xi_j z_2$. We then have

$$a(z_1 z_2^{-1})^{q+1} + (z_1 z_2^{-1})^q + (z_1 z_2^{-1}) + aN(a^{-1})(\text{Tr}(a) - 2a) = 0$$

which is equivalent to

$$(a - 1)(z_1 z_2^{-1})^{q+1} + (z_1 z_2^{-1} + 1)^{q+1} + aN(a^{-1})(\text{Tr}(a) - 2a) - 1 = 0.$$

Since $q + 1$ is even and $z_2 \neq 0$, we can rewrite this equation as

$$(a - 1)z_1^{q+1} + (aN(a^{-1})(\text{Tr}(a) - 2a) - 1)z_2^{q+1} + (-z_1 - z_2)^{q+1} = 0. \quad (2)$$

If we let $z_3 = -z_1 - z_2$, then from the definition of f , g , and h , we have from (2) that

$$f(z_1) + g(z_2) + h(z_3) = 0.$$

Observe that z_1 , z_2 , and z_3 are all non-zero since $\xi_j \notin \{0, -1\}$. Thus, for any $(x, y) \in \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}$, the vertices

$$(x, y)_A, (x + z_1, y + f(z_1))_B, (x + z_1 + z_2, y + f(z_1) + g(z_2))_C$$

form a triangle since

$$(x, y)_A = (x + z_1 + z_2 + z_3, y + f(z_1) + g(z_2) + h(z_3))_A.$$

There are $q + 1$ choices for ξ_j , $q^3 - 1$ choices for z_2 (which then determines z_1 and z_3), and q^6 choices for (x, y) . Altogether, this gives $q^6(q^3 - 1)(q + 1)$ triangles in $G_q(a)$ completing the proof of Theorem 3.1. \blacksquare

We make some final remarks. Constructions using planar monomials and similar to the one used to prove Theorem 1.3 have appeared elsewhere. Allen, Keavash, Sudakov, and Verstraëte [1] use the planar monomial X^2 over \mathbb{F}_q to construct $\{K_3, K_{2,3}\}$ -free graphs with many edges. Other instances include [11] and [12], but like [1], these papers all use X^2 . Using the planar monomial X^2 in place of

X^{q+1} in our construction only leads to an improvement upon the lower bound of Proposition 1.2 by a constant factor of 2. One of the novelties of our approach is the use of a planar polynomial that is more complicated than X^2 . We are not aware of another instance in extremal graph theory where an existing result was improved upon by considering planar polynomials other than X^2 . There is one further class of planar monomials known – the monomial $X^{(3^\alpha+1)/2}$ is planar over \mathbb{F}_{3^e} if and only if $\gcd(\alpha, 2e) = 1$, see [4]. Computational evidence suggests replacing X^{q+1} with these polynomials will not provide an improvement to Theorem 1.3.

4 Acknowledgment

The third listed author would like to thank Jacques Verstraëte and Jason Williford for helpful discussions.

References

- [1] P. Allen, P. Keevash, B. Sudakov, J. Verstraëte, Turán numbers of bipartite graphs plus an odd cycle, *J. Combin. Theory Ser. B* 106 (2014), 134–162.
- [2] N. Alon and C. Shikhelman, Many T copies in H -free graphs, *J. Combin. Theory Ser. B* 121 (2016), 146–172.
- [3] B. Bollobás, E. Györi, Pentagons vs. triangles, *Discrete Math.* 308 (2008), no. 19, 4332–4336.
- [4] R. Coulter, R. Matthews, Planar functions and planes of Lenz-Barlotti Class II, *Des. Codes Cryptogr.* 10 (1997), no. 2, 167–184.
- [5] P. Dembowski, T. G. Ostrom, Planes of order n with collineation groups of order n^2 , *Math. Z.* **103** 1968 239–258.
- [6] P. Fischer, J. Matoušek, A lower bound for families of Natarajan dimension d , *J. Combin. Theory Ser. A* 95 (2001), no. 1, 189–195.
- [7] A. Grzesik, On the maximum number of five-cycles in a triangle-free graph, *J. Combin. Theory Ser. B* 102 (2012), no. 5, 1061–1066.
- [8] E. Györi and H. Li, The maximum number of triangles in C_{2k+1} -free graphs, *Combin. Probab. Comput.* 21 (2012), no. 1-2, 187–191.
- [9] H. Hatami, J. Hladký, D. Král’, N. Serguei, A. Razborov, On the number of pentagons in triangle-free graphs, *J. Combin. Theory Ser. A* 120 (2013), no. 3, 722–732.
- [10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).
- [11] C. Timmons, J. Verstraëte, A counterexample to sparse removal, *European J. Combin.* 44 (2015), part A, 77–86.
- [12] C. Timmons, On r -uniform linear hypergraphs with no Berge- $K_{2,t}$, arXiv: 1609.03401v1 2016.